Phillip S. Ferguson, No. 1063
Barton H. Kunz, II, No. 8827
CHRISTENSEN & JENSEN, P.C.
15 West South Temple, Suite 800
Salt Lake City, UT 84101
Telephone: (801) 323-5000
Facsimile: (801) 355-3472
Email: phillip.ferguson@chrisjen.com
bart.kunz@chrisjen.com

Counsel for Plaintiff Fallon Community Health Plan, Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH, CENTRAL DIVISION

FALLON COMMUNITY HEALTH PLAN, INC., **Plaintiff,** **v.** **BLUEHOST, INC.,** **Defendant.**	**COMPLAINT** **INJUNCTIVE RELIEF REQUESTED** **Civil Case No. 2:09-cv-538** **Judge Ted Stewart**

Plaintiff Fallon Community Health Plan, Inc. ("FCHP"), for cause of action against Bluehost, Inc. ("Bluehost"), alleges as follows:

PARTIES AND JURISDICTION

1. FCHP is a corporation organized under the laws of the Commonwealth of Massachusetts with its principal place of business at 10 Chestnut Street, Worcester, Massachusetts 01608.

2. Defendant Bluehost is a corporation organized under the laws of the State of Utah with its principal place of business at 1215 N. Research Way, No. Q3500, Orem, UT 84097, United States.

3. This Court has jurisdiction over this matter pursuant to its federal question jurisdiction under 28 U.S.C § 1331 in that the matter arises under the laws of the United States (18 U.S.C. § 1030, *et seq.*; 18 U.S.C. § 2510, *et seq.*; and 18 U.S.C. § 2701, *et seq.*), and pursuant to its diversity jurisdiction under 28 U.S.C § 1332 in that plaintiff and defendant are citizens of different states and the amount in controversy exceeds $75,000. This Court has jurisdiction over the state law claims pursuant to its supplemental jurisdiction under 28 U.S.C. § 1367(a) because the state law claims are so related to the claims within the original jurisdiction of this Court that they form part of the same case or controversy.

4. Venue is proper in this District pursuant to 28 U.S.C. § 1391 in that the defendant is a resident of, and may be found within, this District and because a substantial portion of the events giving rise to the claims occurred here.

INTRODUCTION

5. By this action, FCHP seeks to recover certain electronic data unlawfully being held by Bluehost and damages resulting from Bluehost's unlawful actions and gross negligence. In the absence of injunctive relief plaintiff FCHP will suffer irreparable harm not compensable by monetary damages.

BACKGROUND

6. FCHP is in the business of providing health care benefits in the Commonwealth of Massachusetts, including health care plans for groups and individuals.

7. In order to provide these services, FCHP collects personal information, including personal health, identifying, and financial information, from its employees, its clients, their employees and family members. Accordingly, FCHP's electronic information systems contain confidential and sensitive information.

8. Bluehost is in the business of operating computer servers which are repositories for electronic data stored on behalf of its customers.

9. Bluehost currently hosts in excess of 825,000 domains on an unknown number of servers. Bluehost provides web hosting plans with "hacker friendly" features such as SSH (Secure Shell Access), SSL, FTP, CGI, Ruby (RoR), Perl, PHP, MySQL. These services offer an ideal platform for hackers, both foreign and domestic, to launch cyber-attacks against U.S. entities such as FCHP .

10. Beginning on or about late April 2009, parties unknown but believed to be located in the Peoples Republic of China surreptitiously, and by means of a Bluehost server, illegally "hacked" or, more specifically, launched a computer worm that infected over 400 computer systems operated by FCHP and extracted from such systems certain electronic data and information which is the property of FCHP or which FCHP held on behalf of its employees and customers (the "Electronic Property").

11. On or about May 4, 2009, FCHP began to experience difficulties with a large number of desktop computers and, after a review of the firewall logs, discovered unusual network traffic involving an IP address allocated to Bluehost.

12. FCHP retained the services of Lighthouse Computer Services, a computer security and forensic consultancy, that discovered spyware and viruses on approximately 400 company computers. The virus was identified as **W32.Qakbot**. At the time of discovery, the

virus was a zero-day worm that spreads through network shares and opens a back door on compromised computers. Among other functionality, the virus steals information and downloads files on the compromised computer to a server controlled by the hacker.

13. Based on forensic analysis of infected systems it was determined that the virus: (a) logs all keystrokes of a user, including passwords, security codes, and other sensitive data; (b) obtains visited URLs from Internet Explorer browser history (which, in combination with keystroke logging, provides the hacker both the URLs of the websites and the username passwords associated with said websites); (c) obtains Outlook Email user IDs and passwords; (d) obtains user IDs and passwords for File Transfer Protocol ("FTP") sessions accessed by the compromised user's computer; (e) obtains cookies and computer cache information; and (f) obtains the IP address, DNS, and hostnames of the compromised hosts thereby providing valuable data to the hacker to permit the mapping of FCHP's internal network environment to assist with future attacks.

14. The referenced virus collected information as detailed in paragraph 13 (above) including user names and passwords from the compromised computers and sent this data to a remote computer at Bluehost using an Internet communications protocol known as "FTP."

15. Based on information and belief, Bluehost does not provide adequate and appropriate security for hosted accounts, and markets itself to an international clientele with a propensity for nefarious activity. By and through Bluehost's willful disregard, one or more of its servers were compromised and served as a platform to attack FCHP. One of more of Bluehost's servers also served as a data repository for the Electronic Property of FCHP remotely transferred by a computer virus from over 400 infected FCHP computers.

16. On May 4, 2009 alone, between the hours of 10 a.m. (EST) and 8 p.m. (EST), approximately 7,983 individual files containing sensitive data (of the type described in paragraph 13) were collected by the virus and transferred via FTP to a server owned and operated by Bluehost.

17. The Bluehost server in question was assigned the IP address 74.220.207.164. This IP address belongs to an IP range assigned to Bluehost. The IP range assigned to Bluehost is 74.220.192.0 - 74.220.223.255. The domain name of the attacking server, owned and operated by Bluehost, is bengriffmotorsports.com.

18. Despite FCHP's immediate concern and request for assistance from Bluehost with respect to the use of Bluehost's servers as a proxy for attacks originating from mainland China, Bluehost refused to cooperate in assessing the scope of the compromise, the significance of this cyber attack, and/or mitigate damages resulting from this unauthorized transfer of FCHP data from FCHP computers to Bluehost's server.

19. Based on an internal investigation by FCHP and its outside computer security consultant, a subset of the files transferred was sampled. The sampled data included sensitive personal information including Social Security Numbers, Credit Card Numbers, Bank Account Numbers, and other personal information.

20. Bluehost knew, or by the exercise of due diligence and reasonable caution would have known, that it was participating in an enterprise engaged in a pattern of racketeering activity. Its conduct was willful, malicious, and manifested a knowing and reckless indifference toward and disregard of FCHP's rights.

21. As a result of the conduct complained of herein, FCHP has suffered and will continue to suffer irreparable harm not compensable by monetary damages alone.

COUNT I

VIOLATIONS OF THE COMPUTER FRAUD AND ABUSE ACT

(18 U.S.C. §1030 et. seq.)

22. FCHP re-alleges and incorporates herein by reference as though set forth in full each and every allegation contained in Paragraphs 1 through 21 inclusive.

23. In connection with its business, FCHP owns and maintains one or more "protected computers" as defined in the Computer Fraud and Abuse Act, through which sensitive data transmissions are received, stored, and disseminated in interstate and/or foreign commerce or communication.

24. FCHP is informed and believes, and based thereon alleges, that in the two months preceding the date of the filing of this Complaint, Bluehost has either intentionally, or by virtue of its gross negligence, repeatedly participated in a scheme to transmit FCHP's employees', patients', and enrollees' sensitive information without authorization, using FCHP's information systems, causing losses to the Plan of not less than $75,000.

25. FCHP is informed and believes, and based thereon alleges, that Bluehost (and/or its clients in conjunction with it) has intentionally accessed FCHP's protected computer facilities without authorization and to cause harm to the Plan.

26. WHEREFORE, Bluehost has violated the federal Computer Fraud and Abuse Act (18 U.S.C. §1030 *et seq*,) and has caused damage to FCHP including but not limited to the impairment of the integrity and/or availability of data, programs, systems, and/or information in FCHP's protected computer facilities and loss of its Electronic Property, entitling the Plan, inter *alia*, to injunctive relief pursuant to 18 U.S.C. § 1030(g)

COUNT II

FEDERAL WIRETAP ACT (18 U.S.C. § 2510 *et seq.*)

27. FCHP re-alleges and incorporates herein by reference, as though set forth in full, each and every allegation contained in Paragraphs 1 through 26 inclusive.

28. FCHP alleges that Bluehost either installed, or by virtue of Bluehost's own gross negligence caused to be installed, a Trojan-Horse program on FCHP's computers that among other things detects and steals passwords by gathering the passwords from the compromised computer and sending them to a remote computer using an Internet communication protocol called FTP.

29. FCHP uses its computers in connection with its business and the computers are connected to the Internet by typical means.

30. The virus program referred to herein collected information contemporaneous to its transmission over the Internet.

31. WHEREFORE Bluehost has violated the federal Wiretap Act, 18 U.S.C. § 2510 *et seq.*, and has caused damage to FCHP, including but not limited to the impairment of the integrity and/or availability of data, programs, systems, and/or information in FCHP's protected computer facilities and loss of its Electronic Property

COUNT III

THE STORED COMMUNICATIONS ACT (18 U.S.C. § 2701, *et seq.)*

32. FCHP re-alleges and incorporates herein by reference, as though set forth in full, each and every allegation contained in Paragraphs 1 through 31 inclusive.

33. FCHP operates as an electronic communications services provider in its capacity as a company providing health benefits by providing Internet-based applications to its customers,

employees, and potential customers. In addition, FCHP operates an email system for use by its employees who can remotely access said information system from anywhere in the world.

34. Bluehost directly or indirectly transmitted and/or caused the virus and instructions to the virus to be communicated over the Internet to FCHP computers, and thereby targeted passwords which were system passwords saved on the users' hard drives, as well as web-based passwords, for capture during transmission over the internet.

35. The files accessed by the virus were stored with FCHP, an electronic service provider under the terms of 18 U.S.C. § 2701, *et seq.*

36. WHEREFORE, Bluehost has violated the federal Stored Communications Act, 18 U.S.C. § 2710 *et seq*., and has caused damage to FCHP, including but not limited to the impairment of the integrity and/or availability of data, programs, systems, and/or information in FCHP's protected computer facilities, and loss of its Electronic Property.

COUNT IV

CONVERSION

37. FCHP re-alleges and incorporates herein by reference as though set forth in full each and every allegation contained in Paragraphs 1 through 36 inclusive.

38. The Electronic Property referred to herein is the property of FCHP.

39. Bluehost, without lawful justification, willfully and repeatedly participated in a scheme to obtain FCHP's property by transmitting FCHP's electronic data containing sensitive information about its company, employees, patients, and enrollees.

WHEREFORE, Bluehost has unlawfully and tortiously converted the property of FCHP and has caused damage to FCHP, including but not limited to the impairment of the integrity

and/or availability of data, programs, systems, and/or information in FCHP's protected computer facilities and loss of its Electronic Property.

COUNT V

REPLEVIN

40. FCHP re-alleges and incorporates herein by reference as though set forth in full each and every allegation contained in Paragraphs 1 through 39 inclusive.

41. Bluehost's interference and transmittal of FCHP's data, including sensitive confidential information, deprives FCHP of the Electronic Property to which it is lawfully and immediately entitled.

42. WHEREFORE, FCHP is entitled to a common law writ of replevin to require Bluehost to immediately return to FCHP all FCHP's Electronic Property which it unlawfully possesses. This Court has authority to issue such writ pursuant to Rule 64 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

WHEREFORE, FCHP requests that judgment be entered in its favor and against Bluehost:

A. Granting preliminary and permanent injunctive relief and a writ of replevin requiring Bluehost to return to FCHP all FCHP Electronic Property in its possession;

B. Granting preliminary and permanent injunctive relief requiring Bluehost to delete from its computer servers and elsewhere all FCHP Electronic Property in its

possession and to take such other steps and measures necessary to return FCHP to the *status quo ante*;

C. Awarding FCHP such damages as may be shown by the evidence to have incurred, but in no event less that $75,000;

D. Awarding FCHP punitive damages as authorized by law, including but not limited to Utah Code Annotated § 78B-8-201

E. Granting FCHP such other relief as may be just and proper;

F. Awarding FCHP its costs and expenses of litigation, including reasonable attorney fees.

DATED this 12th day of June, 2009.

CHRISTENSEN & JENSEN, P.C.

/s/ Phillip S. Ferguson
Phillip S. Ferguson
Barton H. Kunz, II

Lee Calligaro
Robert Hudock
EPSTEIN BECKER & GREEN, P.C.
1227 25th Street, N.W.
Suite 700
Washington D.C. 20037
PHONE: (202) 861-0900
FAX: (202) 296-2882

Attorneys for Plaintiff FCHP

Plaintiff's Address:
10 Chestnut Street
Worcester, Massachusetts 01608

Serve: Matthew M. Heaton, President
1215 N. Research Way
No. Q3500
Orem, Utah 84097